Information Security Attacks: Types & Possible Remedies

Ravikar Srivastava
National Informatics Centre, New Delhi

ABSTRACT

Information security is the need of hour today. In the modern world, everything is connected to data communication. We should not forget that intruders are very equipped now and they have tremendous computing strength. Intruders try different ways to retrieve the sensitive information by launching various security attacks. It is very important to understand about these security attacks because it is very essential in order to find out the required solutions. Keeping this problem in mind, in this paper, some security attacks and their possible remedies are discussed briefly so that it will help to design required security solutions.

Keywords**: Information Security, Brute Force, DoS, MITM, Dictionary Attacks**

INTRODUCTION:

As long as information security is concerned, one must understand cryptology, cryptography and cryptanalysis. Cryptography is all about making the information secure. Cryptanalysis is done by intruders for breaking the security by various attacks. Cryptography and cryptanalysis are together known as cryptology as described in the figure below.

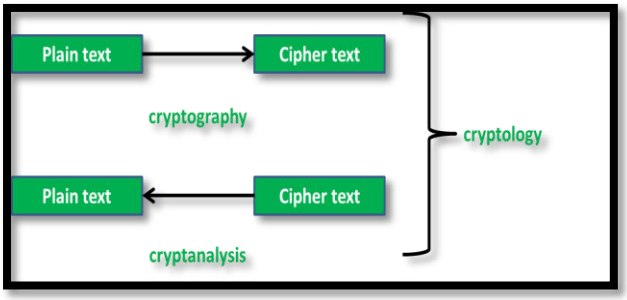

Fig.1. Showing that cryptology includes cryptography and cryptanalysis both

Cryptography hols the responsibility of providing required information security and it provides goals of information security as shown in below figure.

Fig.2. Showing goals of cryptography

Secrecy or confidentiality provides required encryption in order to convert plain text to cipher text so that intruders can't read it. Authentication means participating entities must recognize each other in order to make sure the legitimacy of data. Data integrity makes sure that the received data is not altered by intruders. Non-repudiation makes sure that participating entities can't deny previously made commitments. A study of cryptography and its allied areas [1-9], wireless communication scenarios [10-15] and network security applications [16-20] is very essential to understand various security attacks and possible remedies against them.

POSSIBLE ATTACKS:

Here we talk about some common attacks launched by intruders and they are given as follows:

Dictionary attacks: It is launched by intruders on a password protected systems/networks [21]. All the dictionary words are searched as a possible password. The main reason behind this attack is that many systems or network permits to set ordinary words as passwords. Known phrases and idioms can also be tried in this. There are many tools available for dictionary attacks such as Cain and Abel, Aircrack-ng and John the Ripper etc. The below figure illustrates dictionary attack.

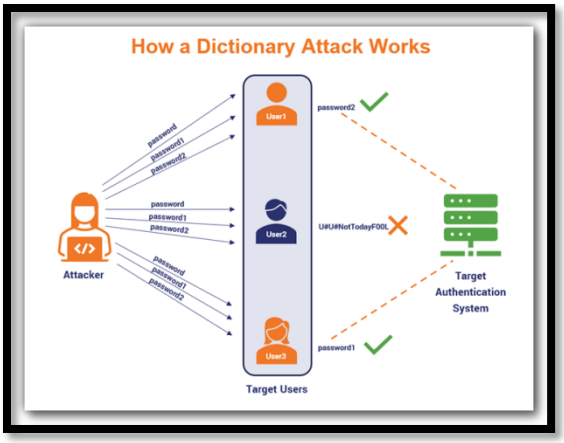

Fig.3. Showing the working of dictionary attack

Brute Force Attack: In this attack, an intruder tries all possible combinations to crack the password [22]. It is computationally very expensive process and as the length of password increases, the required time to crack increases exponentially. This attack is very dangerous for all those users who use weak passwords as it can be cracked very quickly. Using the same password for all multiple usages

is also very dangerous as the success of one brute force will endanger the security of other passwords as well. The below figure illustrates brute force attack.

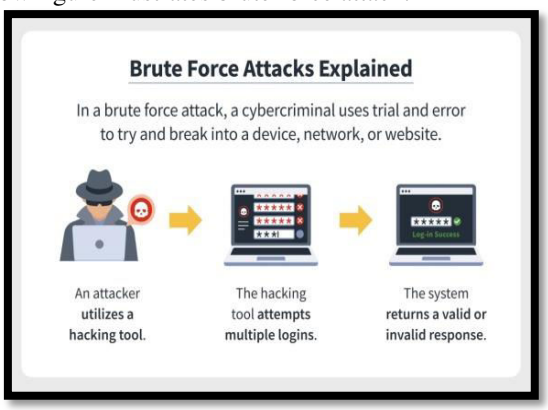

Fig.4. Explaining brute force attack

Man in the Middle Attack (MITM): In this attack an intruder holds a place between transmitter and receiver and the entire communication is then passes through the intruder [23]. Intruder can alter the ongoing communication and holds the capability to provide intentional delay in order to disrupt the ongoing services. MITM can be seen as a type of session hijacking. The below figure illustrates the working of MITM.

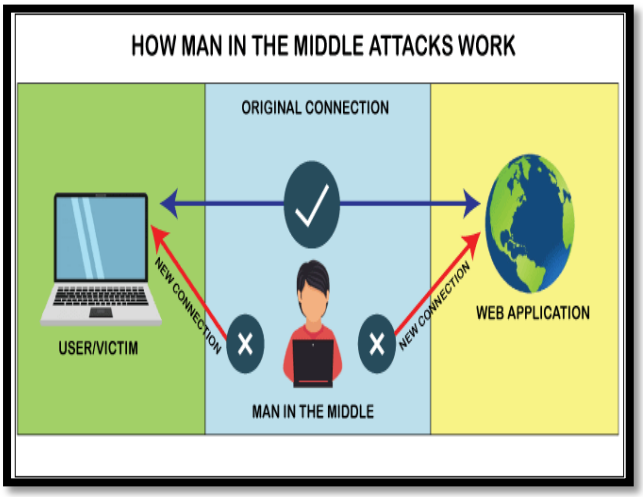

Fig.5. Showing the working of MITM

Denial of Service (DoS) Attack: DoS is launched by an intruder in order to disturb the ongoing resource sharing for legitimate users [24]. DoS can be launched by flooding the target server with traffic and usually e-commerce and banking websites becomes victim of it. It is important to mention here that DoS attacks usually do not responsible for the significant loss of information but they always dent the services with respect to time and loss of business. The below figure illustrates DoS attack.

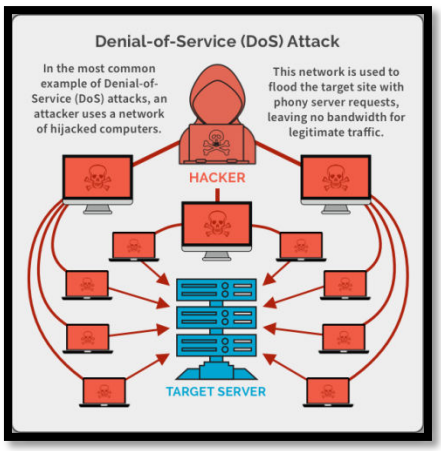

Fig.6. Showing DoS attack

Remedies to Encounter Security Attacks: It is always recommended to adopt certain remedies to avoid the above mentioned attacks. Dictionary attacks can be avoided by carefully selected the password. The password should not be a valid word of English dictionary only. It must be a combination of uppercase, lowercase and special characters. Brute force attack can be avoided by increasing the length of the password and the password must be changed frequently. Multi factor authentication can be incorporated in order to make sure that merely cracking the password will not work for intruders. For example, the two factor authentication process may include user password followed by OTP on the registered mobile number of user. When both the required fields i.e. password with OTP are filled correctly then only the permission will be granted. Strong authentication mechanism on access points is essential for the avoidance of MITM. The use of Virtual Private Network (VPN) is also recommended. Public key encryption is also used to avoid MITM. In public key encryption, a public-private key pair exists. The private key is kept secret by user only and it is not transmitted anywhere. The message can be encrypted by public key which is openly available but decrypted only by the private key held by user only. The below figures illustrate remedies to protect against above mentioned attacks.

Fig.7. Showing possible remedies against brute force attack

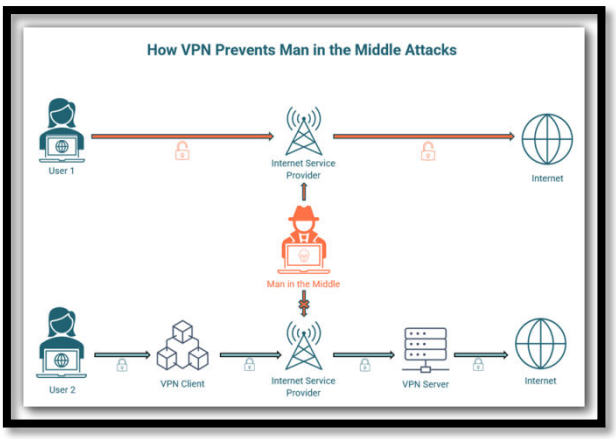

Fig.8. Showing possible remedies against MITM

CONCLUSION & FUTURE SCOPE:

Cryptology includes cryptography and cryptanalysis both. Cryptography provides secrecy, data integrity, authentication and non repudiation and they are called as goals of cryptography or goals of information security. Dictionary attacks, brute force attack are applied on passwords. MITM occurs when an individual holds a place between transmitter and receiver. DoS is launched for degrading overall QoS of the network. The length of the password should be good enough and the password must contain a combination of uppercase, lowercase and special characters. The use of VPN and public key encryption is also recommended to avoid various security attacks.

REFERENCES

[1]. V. Shukla, A. Chaturvedi, N. Srivastava, Nanotechnology and cryptographic protocols: issues and possible solutions, Nanomaterials and energy, volume 8, issue 1, 2019, 1-6,
DOI: 10.1680/jnaen.18.00006

[2]. M.K. Misra, A. Chaturvedi, S.P. Tripathi, V. Shukla, A unique key sharing protocol among three users using non-commutative group for electronic health record system, Journal of discrete mathematical sciences and cryptography, volume 22, issue 8, 2019, 1435–1451,
DOI: 10.1080/09720529.2019.1692450

[3]. A. Chaturvedi, N. Srivastava, V. Shukla, A secure wireless communication protocol using Diffie-Hellman key exchange, International journal of computer applications, volume 126, number 5, 2015, 35-38,
DOI: 10.5120/ijca2015906060

[4]. V. Shukla, A. Chaturvedi, M.K. Misra, On authentication schemes using polynomials over non commutative rings, Wireless personal communications, volume 118, issue 1, 2021, 1-9,
DOI: https://doi.org/10.1007/s11277-020-08008-4

[5]. V. Shukla, A. Mishra, S. Agarwal, A new one time password generation method for financial transactions with randomness analysis, Innovations in electrical and electronic engineering (Part of the lecture notes in electrical engineering book series (LNEE, volume 661)), 2020, 713-720,
DOI: https://doi.org/10.1007/978-981-15-4692-1_54

[6]. V. Shukla, A. Mishra, A. Yadav, An authenticated and secure electronic health record system, IEEE international conference on information and communication technology, 2019, 1-5,
DOI: 10.1109/CICT48419.2019.9066168

[7]. A. Chaturvedi, V. Shukla, M.K. Misra, Three party key sharing protocol using polynomial rings, 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), 2018, 1-5,
DOI: 10.1109/UPCON.2018.8596905

[8]. V. Shukla, A. Chaturvedi, N. Srivastava, Secure wireless communication protocol: to avoid vulnerabilities in shared authentication, Communications on applied electronics, volume 7, number 6, 2017, 4-7,
DOI: 10.5120/cae2017652680

[9]. V. Shukla, M.K. Misra, A. Chaturvedi, Journey of cryptocurrency in India in view of financial budget 2022-23, Cornell university arxiv, 2022, 1-6,
DOI: https://doi.org/10.48550/arXiv.2203.12606

[10]. V. Shukla, N. Srivastava, A. Chaturvedi, A bit commitment signcryption protocol for wireless transport layer security (wtls), IEEE international conference on electrical, computer and electronics engineering , 2016, 83-86,
DOI: 10.1109/UPCON.2016.7894629

[11]. V. Shukla, A. Chaturvedi, N. Srivastava, A new secure authenticated key agreement scheme for wireless (mobile) communication in an EHR system using cryptography, Communications on applied electronics, volume 3, number 3, 2015, 16-21,
DOI: 10.5120/cae2015651903

[12]. A. Chaturvedi, N. Srivastava, V. Shukla, S.P. Tripathi, M.K. Misra, A secure zero knowledge authentication protocol for wireless (mobile) ad-hoc networks, International journal of computer applications, volume 128, number 2, 2015, 36-39,
DOI: 10.5120/ijca2015906437

[13]. V. Shukla, A. Chaturvedi, N. Srivastava, Authentication aspects of dynamic routing protocols: associated problem & proposed solution, International journal of recent technology and engineering, volume 8, issue 2, 2019, 412-419,
DOI: 10.35940/ijrte.B1503.078219

[14]. V. Shukla, A. Kushwaha, S.S. Parihar, S. Srivastava, V. P. Singh, Authenticated wireless information display system using GSM module, Communications on applied electronics, volume 5, number 3, 2016, 7-11,
DOI: 10.5120/cae2016652251

[15]. V. Shukla, A. Chaturvedi, N. Srivastava, Double layer cryptographic protocol for mobile ad-hoc networks (MANETs) by commitment scheme, Communications on applied electronics, volume 7, number 9, 2017, 32-36, DOI: 10.5120/cae2017652716

[16]. V. Shukla, A. Chaturvedi, N. Srivastava, A secure stop and wait communication protocol for disturbed networks, Wireless personal communications, volume 110, 861-872, 2019,
DOI: https://doi.org/10.1007/s11277-019-06760-w

[17]. V. Shukla, A. Mishra, A new sequential coding method for secure data communication, IEEE international conference on computing, power and communication technologies, 2020, 529-533,
DOI: 10.1109/GUCON48875.2020.9231252

[18]. A. Chaturvedi, V. Shukla, M.K. Misra, A random encoding method for secure data communication: an extension of sequential coding, Journal of discrete mathematical sciences and cryptography, volume 24, issue 5, 2021, 1189-1204,
DOI: https://doi.org/10.1080/09720529.2021.1932902

[19]. V. Shukla, A. Chaturvedi, N. Srivastava, A new one time password mechanism for client-server applications, Journal of discrete mathematical sciences and cryptography, volume 22, 2019, 1393-1406,
DOI: 10.1080/09720529.2019.1692447

[20]. V. Shukla, M.K. Misra, A. Chaturvedi, A new authentication procedure for client-server applications using HMAC, Journal of discrete mathematical sciences and cryptography, volume 24, issue 5, 2021, 1241-1256,
DOI: https://doi.org/10.1080/09720529.2021.1932908

[21]. K.H. Hong, B.M. Lee, A deep learning-based password security evaluation model, Applied sciences, volume 12, issue 5, 2022, 1-17,
DOI: https://doi.org/10.3390/app12052404

[22]. R. Hofstede, M. Jonker, A. Sperotto, A. Pras, Flow-based web application brute-force attack and compromise detection, Journal of network and systems management, volume 25, 2017, 735-758,
DOI: https://doi.org/10.1007/s10922-017-9421-4

[23]. A. Mallik, A. Ahsan, M.M.Z. Shahadat, J.C. Tsou, International journal of data and network science, volume 3, issue 2, 2019, 77-92,
DOI: 10.5267/j.ijdns.2019.1.001

[24]. A. Lohachab, B. Karambir, Critical analysis of DDoS-an emerging security threat over IoT networks, Journal of communications and information networks, volume 3, 2018, 57-78,
DOI: https://doi.org/10.1007/s41650-018-0022-5